Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, comprising:

a ~~client~~ module configured to generate a header comprising a plurality of ~~one or more~~ sets of encrypted security information corresponding to respective one of a plurality of groups of users ~~as to who and how a file including the electronic data can be accessed,~~ and configured to generate an encrypted data portion ~~comprising the file~~ encrypted with ~~one or more~~ a plurality of file keys, each of the file keys corresponding to each of the sets ~~according to a predetermined cipher scheme~~, wherein the header is associated with ~~coupled to~~ the encrypted data portion to generate a secured file~~, each set of the one or more sets of encrypted security information associated with a designated group of users~~; and

a ~~server~~ module configured to obtain a respective one of the file keys ~~file key~~ associated with a corresponding one of the plurality of groups ~~the designated group of users~~ and to decrypt ~~only a~~ the set of the plurality of ~~one or more~~ sets of encrypted security information associated with the respective one of the groups ~~designated group of users~~ to allow access by the respective one of the groups ~~designated group of users~~.

2. (Currently Amended) The system as recited in Claim 1, wherein the plurality of ~~one or more~~ sets of encrypted security information in the header of the secured file facilitates the restricted access to the file.

3. (Currently Amended) The system as recited in Claim 1, wherein the plurality of ~~one or more~~ sets of security information is encrypted with a key from the plurality of ~~one or more~~ file keys associated with the one of a plurality of groups ~~the designated group~~ of users.

4. (Currently Amended) The system as recited in Claim 3, wherein the one of a plurality of groups ~~the designated group~~ of users ~~is~~ includes one or more of ~~selected from a group consisting~~ of ~~a~~ human users, ~~a~~ software agents, and ~~a~~ devices ~~and a group of users~~; and wherein the one of a plurality of groups ~~the designated group~~ of users is granted access privilege to access the file.

5. (Currently Amended) The system as recited in Claim 4, wherein the plurality of ~~one or more~~ sets of encrypted security information comprises one of the plurality of ~~the~~ file keys and access rules to ~~the~~ restricted access to the file.

6. (Currently Amended) The system as recited in Claim 5, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when the access privilege of the one of a plurality of groups ~~the designated group~~ of users is ~~within~~ consistent with access permissions by the access rules.

7. (Previously Presented) The system as recited in Claim 6, wherein the access rules are expressed in a markup language.

8. (Previously Presented) The system as recited in Claim 7, wherein the markup language is Extensible Access Control Markup Language.

9. (Currently Amended) The system as recited in Claim 7, wherein the markup language ~~is~~ includes one or more ~~selected from a group consisting~~ of HTML, XML, and SGML.

10. (Previously Presented) The system as recited in Claim 1, wherein the secured file is configured to have a file extension identical to what the file originally has so that an application designated to access the file can be executed to access the secured file.

11. (Currently Amended) The system as recited in Claim 10, wherein each of the plurality of ~~one or more~~ sets of encrypted security information comprises a flag to the application that the secured file being accessed can not be accessed as it is normally accessed ~~does~~.

12. (Previously Presented) The system as recited in Claim 11, wherein the flag is configured to be placed in a position of the secured file so that the flag will be accessed first when the secured file is accessed by the application.

13. (Currently Amended) The system as recited in Claim 10, wherein each of the plurality of ~~one or more~~ sets of encrypted security information comprises the file key and access rules, the access rules controlling who and how the secured file can be accessed, and wherein the security information in the header is organized in such a way that the application is paused, upon detecting that the secured file is being accessed, for an access control module to determine whether the one of a plurality of groups ~~the designated group~~ of users requesting the secured file has proper access privileges to do so with respect to the access rules in the security information.

14. (Previously Presented) The system as recited in Claim 13, wherein the access control module operates in a path through which the secured file is confined to be loaded into the application.

15. (Previously Presented) The system as recited in Claim 1, wherein the file key is a symmetric cipher key.

16. (Currently Amended) The system as recited in Claim 1, wherein the electronic data ~~file~~ is one or more of an electronic document, a multimedia file, ~~a set of~~ dynamic or static data, ~~a sequence of~~ executable code, an image file, streaming audio, streaming video, executable code, audio files, databases, database tables, database table records, collections of electronic files; and collections of electronic documents ~~and a text data~~.

17. (Currently Amended) A system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, comprising:

a ~~client~~ module configured to generate a header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data, wherein N >=1 and an encrypted data portion including the electronic data encrypted according to a predetermined cipher; and

wherein the header is associated with ~~coupled to~~ the encrypted data portion to generate a secured file, and the file key can be retrieved to decrypt the encrypted data portion only when the access rules in one of the N encrypted segments are measured successfully against access privileges associated with a group of designated users accessing the secured file.

18. (Previously Presented) The system as recited in Claim 17, wherein the header further comprises a user block having user information identifying who can access the secured file.

19. (Previously Presented) The system as recited in Claim 17, wherein each of the N encrypted segments of the rule block comprises policies on how the secured file can be accessed.

20. (Previously Presented) The system as recited in Claim 18, wherein the user block includes N encrypted segments, each including the file key.

21. (Previously Presented) The system as recited in Claim 20, wherein each of the N encrypted segments of the user block corresponds to one of the N encrypted segments of the rule block.

22. (Previously Presented) The system as recited in Claim 20, wherein each of the N encrypted segments of the user block further comprises a user identification identifying who can access the secured document.

23. (Previously Presented) The system as recited in Claim 20, wherein each of the N encrypted segments of the user block further comprises cipher information about the predetermined cipher to facilitate a decryption process of the encrypted data portion with the file key.

24. (Previously Presented) The system as recited in Claim 20, wherein the access rules in each of the N encrypted segments of the rule block determine at least an action with which the secured document can be accessed by the designated group of users associated with one of the N encrypted segments of the user block.

25. (Currently Amended) The system as recited in Claim 24, wherein the action comprises one or more of ~~commands:~~ open, export, read, edit, play, listen to, or print ~~or forward and attach~~.

26. (Previously Presented) The system as recited in Claim 20, wherein the access rules in each of the N encrypted segments of the rule block are expressed in a markup language.

27. (Previously Presented) The system as recited in Claim 26, wherein the markup language is Extensible Access Control Markup Language.

28. (Currently Amended) The system as recited in Claim 26, wherein the markup language is one or more ~~selected from a group consisting~~ of HTML, XML, and SGML.

29. (Previously Presented) The system as recited in Claim 20, wherein the N encrypted segments of the user block are respectively encrypted with the file key.

30. (Previously Presented) The system as recited in Claim 29, wherein an authorized designated group of users associated with one of the encrypted segments of the user block can view the access rules of each of the N encrypted segments of the rule block when access privilege of the authorized designated group of users is measured successfully with the access rules in one of the N encrypted segments in the rule block associated with the authorized designated group of users.

31. (Previously Presented) The system as recited in Claim 30, wherein the authorized designated group of users can update the access rules of each of the N encrypted segments of the rule block.

32. (Previously Presented) The system as recited in Claim 20, wherein the N encrypted segments of the user block remain encrypted every time the secured file is stored in a storage space.

33. (Currently Amended) In a system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, a method for generating the format, comprising:

obtaining a file key;

encrypting the electronic data with the file key according to a predetermined cipher to produce an encrypted data portion; and

integrating a header comprising a plurality of ~~one or more~~ sets of encrypted security information with the encrypted data portion to generate a secured file, wherein the encrypted security information comprises the file key and access rules to control the restricted access to the electronic data in the secured file, each set of the plurality of ~~one or more~~ sets of encrypted security information associated with a corresponding one of a plurality of groups ~~a designated group~~ of users.

34. (Currently Amended) The method of Claim 33, wherein the encrypted security information comprises user information as to which of the corresponding one of a plurality of groups ~~a designated group~~ of users can access the secured file.

35. (Currently Amended) The method of Claim 34, wherein the plurality of ~~one or more~~ sets of encrypted security information can only be decrypted by a key associated with the corresponding one of a plurality of groups ~~a designated group~~ of users identified in the user information in the plurality of ~~one or more~~ sets of encrypted security information.

36. (Currently Amended) The method of Claim 34, wherein the corresponding one of a plurality of groups ~~a designated group~~ of users includes one or more ~~is a member selected from a group consisting~~ of ~~a~~ human users, ~~a~~ software agents, and ~~a~~ devices ~~and a group of users~~; and wherein the users are ~~is~~ granted access privileges to access the secured file.

37. (Currently Amended) The method of Claim 36 further comprising obtaining the access rules from either a default setting for a file place in which the secured file is to be placed or a manual setting in accordance with access privilege associated with a user from the corresponding one of a plurality of groups ~~a designated group~~ of users who is creating the secured file.

38. (Original) The method of Claim 33, wherein the obtaining of the file key comprises:

if the secured file is newly generated, generating the file key from the predetermined cipher; and if the secured file is being stored in a storage place, retrieving the file key from a memory store; and

deleting the file key from a memory store as soon as the secured file is stored in the storage place.

39. (Currently Amended) The method of claim 1, wherein each of the corresponding one of a plurality of groups ~~a designated group~~ of users has different access privileges.